

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-087289

(43)Date of publication of application : 20.03.2003

(51)Int.Cl.

H04L 12/46

H04L 12/28

H04Q 7/38

(21)Application number : 2001-278283

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 13.09.2001

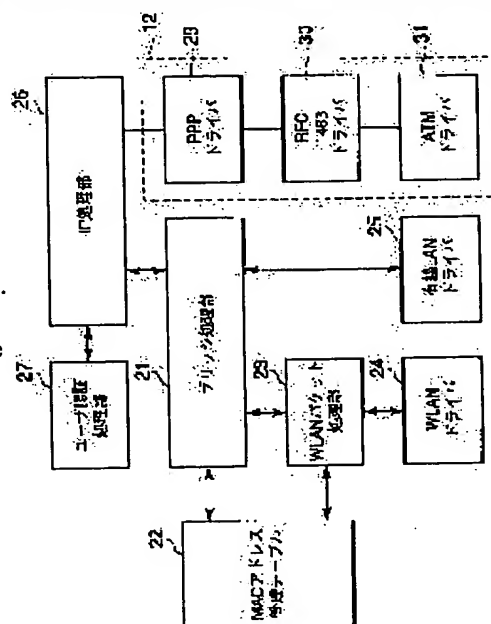
(72)Inventor : KOBAYASHI TAKEAKI
ISHIBASHI YASUHIRO

(54) ELECTRONIC EQUIPMENT HAVING RELAY FUNCTION FOR RADIO DATA COMMUNICATION

(57)Abstract:

PROBLEM TO BE SOLVED: To realize various communication service functions by an operation for changing-over communication services through the use of the enciphering function of a radio communication packet.

SOLUTION: An access point is provided with a function for checking existence of application of an enciphering function (WEP) at every radio communication packet and deciding the packet communication service based on the application state. The access point is provided with a wireless LAN packet processing part 23 including a function for checking presence of application of WEP in a reception packet from a radio terminal.



PU030121
 CITED BY APPLICANT

Amended to US 2003/0051132

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2003-87289
(P2003-87289A)

(43) 公開日 平成15年3月20日 (2003.3.20)

(51) Int.Cl. ⁷	識別記号	F I	テ-マコ-ト* (参考)
H 0 4 L 12/46		H 0 4 L 12/46	Z 5 K 0 3 3
12/28	3 0 0	12/28	3 0 0 Z 5 K 0 6 7
H 0 4 Q 7/38		H 0 4 B 7/26	1 0 9 R

審査請求 有 請求項の数14 O L (全 8 頁)

(21) 出願番号 特願2001-278283(P2001-278283)

(22) 出願日 平成13年9月13日 (2001.9.13)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 小林 丈朗

東京都青梅市末広町2丁目9番地 株式会
社東芝青梅工場内

(72) 発明者 石橋 泰博

東京都青梅市末広町2丁目9番地 株式会
社東芝青梅工場内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外6名)

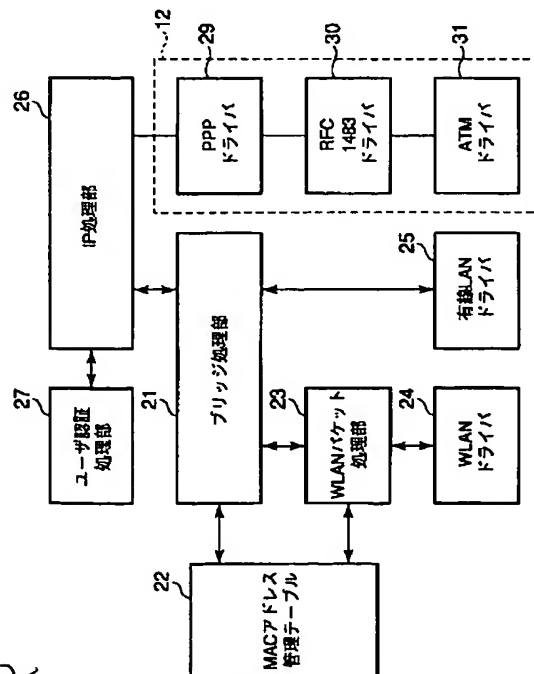
最終頁に続く

(54) 【発明の名称】 無線データ通信の中継機能を有する電子機器

(57) 【要約】

【課題】無線通信パケットの暗号化機能を利用して、通信サービスの切替え運用による多様な通信サービス機能を実現することにある。

【解決手段】無線通信パケット毎に、暗号化機能 (W E P) の適用の有無をチェックし、当該適用状態に基づいてパケットの通信サービスを決定できる機能を備えたアクセスポイントに関する。当該アクセスポイントは、無線端末からの受信パケットにW E Pの適用の有無をチェックする機能を有する無線LANパケット処理部23を備えている。



14030121
correcto
us 2003/0051132

【特許請求の範囲】

【請求項 1】 無線通信機能を有する端末装置と、前記端末装置と他の通信機器との間のデータ通信の中継機能を有する電子機器において、
前記端末装置と無線通信を行なう無線部と、
前記無線部を介して前記端末装置から送信された通信データが暗号化されているか否かを判断する手段と、
前記判断手段の判断結果に基づいて、前記通信データを送信する送信先を制限する通信処理手段とを具備したことを特徴とする電子機器。

【請求項 2】 前記判断手段は、前記端末装置から送信された通信データがパケット単位で暗号化されているか否かを判断し、
前記通信処理手段は、前記パケット単位で前記通信データの中継先を制限することを特徴とする請求項 1 に記載の電子機器。

【請求項 3】 前記通信処理手段は、前記暗号化機能が非適用のパケットの場合には、当該パケットを通信不能として破棄するように構成されていることを特徴とする請求項 1 に記載の電子機器。

【請求項 4】 前記電子機器は、さらに有線 LAN に接続する通信ポートを具備し、
前記通信処理手段は、前記通信データが暗号化されていない時には、前記通信データを前記通信ポートへ送信することを禁止することを特徴とする請求項 1 または請求項 2 に記載の電子機器。

【請求項 5】 前記電子機器は、さらに有線 LAN に接続する第 1 の通信ポートと、外部の一般公衆回線網に接続する第 2 の通信ポートとを具備し、
前記通信処理手段は、前記通信データが暗号化されていない時には、前記通信データを前記第 2 の通信ポートへ送信することを禁止し、前記第 1 の通信ポートへ前記通信データを送信することを許可することを特徴とする請求項 1 または請求項 2 に記載の電子機器。

【請求項 6】 前記通信処理手段は、前記暗号化機能が非適用のパケットの場合には、通信プロトコルの種類を制限するように構成されていることを特徴とする請求項 1 に記載の電子機器。

【請求項 7】 前記通信処理手段は、前記暗号化機能が非適用のパケットの場合に、当該パケットが認証処理に関係するデータを含む場合のみ通信を許可し、それ以外のデータを含む場合には当該パケットを破棄するように構成されていることを特徴とする請求項 1 に記載の電子機器。

【請求項 8】 前記通信ポートは、無線 LAN、有線 LAN、あるいはインターネットを含む WAN のそれぞれに接続するための通信ポートであることを特徴とする請求項 1 から請求項 7 のいずれか 1 項に記載の電子機器。

【請求項 9】 無線通信機能を有する端末装置と、前記端末装置との間で無線データ通信の中継機能を備えた電

子機器に適用する通信処理方法において、
前記端末装置から送信されるパケット単位のデータを受信するステップと、
前記受信ステップにより受信されたパケットに無線通信用の暗号化機能が適用されているか否かを判別するステップと、
前記判別手段の判別結果に基づいて、パケットの取り扱いを決定するステップとからなることを特徴とする通信処理方法。

10 【請求項 10】 無線通信機能を有する端末装置と、前記端末装置との間で無線データ通信の中継機能を備えた電子機器に適用する通信処理方法において、
前記端末装置から送信されるパケット単位のデータを受信するステップと、
前記受信ステップにより受信されたパケットに無線通信用の暗号化機能が適用されているか否かを判別するステップと、
前記判別ステップの判別結果に基づいて、前記暗号化機能が非適用のパケットの場合には当該パケットを通信不能として破棄し、前記暗号化機能が適用されたパケットの場合には所定の通信処理を実行するステップとからなることを特徴とする通信処理方法。

20 【請求項 11】 無線通信機能を有する端末装置と、前記端末装置との間で無線データ通信の中継機能を備えた電子機器に適用する通信処理方法において、
前記端末装置から送信されるパケット単位のデータを受信するステップと、
前記受信ステップにより受信されたパケットに無線通信用の暗号化機能が適用されているか否かを判別するステップと、
前記判別ステップの判別結果に基づいて、前記暗号化機能が非適用のパケットの場合には有線 LAN に接続した通信ポートへ当該パケットを転送することを禁止し、前記暗号化機能が適用されたパケットの場合には転送可能な通信ポートへの転送を実行するステップとからなることを特徴とする通信処理方法。

30 【請求項 12】 無線通信機能を有する端末装置と、前記端末装置との間で無線データ通信の中継機能を備えた電子機器に適用する通信処理方法において、
前記端末装置から送信されるパケット単位のデータを受信するステップと、
前記受信ステップにより受信されたパケットに無線通信用の暗号化機能が適用されているか否かを判別するステップと、
前記判別ステップの判別結果が暗号化機能が非適用である場合に、当該パケットが認証処理に関係するデータを含む場合には当該パケットの通信を許可し、それ以外のデータを含む場合には当該パケットを破棄するステップとからなることを特徴とする通信処理方法。

50 【請求項 13】 無線通信機能を有する端末装置と、前

記端末装置と他の通信機器との間のデータ通信の中継機能を有する電子機器において、
前記端末装置と無線通信を行なう無線部と、
前記端末装置以外の機器と通信を行なうための第1の通信手段と、
前記端末装置以外の機器と通信を行ない、前記第1の通信手段とは異なる第2の通信手段と、
前記無線部を介して前記端末装置から送信された通信データが暗号化されているか否かを判断する手段と、
前記判断手段により前記通信データが暗号化されていると判断した場合、前記通信データを前記第1の通信手段へ送信することを禁止し、前記第2の通信手段を介して前記通信データを前記第2の通信手段へ送信することを許可する通信処理手段とを具備したことを特徴とする電子機器。

【請求項14】 前記判断手段は、前記端末装置から送信された通信データを、パケット単位で暗号化されているか否かを判断し、
前記通信処理手段は、前記パケット単位で前記通信データの中継先を制限することを特徴とする請求項13に記載の電子機器。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、一般的には無線端末装置とネットワークとの中継機能を有する電子機器に関し、特に無線通信パケットのセキュリティ状態を監視する機能を備えたアクセスポイントの技術に関する。

【0002】

【従来の技術】近年、IEEE802.11による無線LAN規格を代表とする無線ネットワークの構築が推進されている。この無線ネットワークは、複数の無線端末とアクセスポイント（access point、以下APと呼ぶ場合がある）と呼ぶネットワーク接続装置とから構成される。無線端末は、無線通信機能を有する端末装置、具体的にはパーソナルコンピュータや、携帯電話機も含むモバイル情報機器（PDA）等に相当する。APは、パーソナルコンピュータなどの端末装置と基幹ネットワークとの中継機能を有し、さらに具体的に言うと、パーソナルコンピュータと無線通信を行ない、そのデータを基幹ネットワークである有線LANへ中継する。またその逆の機能も有する。

【0003】アクセスポイントは、ESSID（extended service set identity）と呼ぶ複数のアクセスポイントのグループを識別するためのID情報を、周辺の各無線端末に通知する機能を有する。無線端末は、アクセスポイントが通知するESSIDを利用して、所望のアクセスポイントに接続できる。このような仕組みにより、無線端末は、アクセスポイントに無線通信で接続し、所望の無線LANとのデータ通信を行なうことができる。

【0004】ところで、IEEE802.11による無線LAN規格のオプション機能として、WEP（wired equivalent privacy）と呼ばれるデータパケット（無線通信パケット）の暗号化機能が規定されている。このWEP機能を利用する場合には、ESSIDとWEPの設定とを相互に一致するように設定することにより、無線端末が、所望のアクセスポイントに接続できることになる。

【0005】要するに、アクセスポイントがWEP適用状態に設定された場合には、無線端末（無線LANにアクセス可能な端末）もWEP適用状態に設定される必要がある。逆に、アクセスポイントがWEPの非適用状態であれば、無線端末もWEPの非適用状態であることが要求される。但し、アクセスポイントにWEP適用状態が設定されている場合でも、WEP非適用の状態、無線端末との通信を実行する機能を備えたアクセスポイントを構築することは可能である。

【0006】

【発明が解決しようとする課題】WEPの適用とは、パケットのデータを暗号化して、無線端末とアクセスポイント間の無線通信におけるデータのセキュリティ（第三者による傍受の回避機能）を高めることである。無線LANのセキュリティは重要であるため、WEPを適用したアクセスポイントの運用が一般的である。しかし一方で、必ずしも高度のセキュリティを必要としない通信サービスの需要も多い。

【0007】従って、WEPの適用または非適用のいずれの無線通信パケットを取り扱うことができるアクセスポイントの運用が望ましい。しかしながら、従来では、WEPの適用または非適用に応じて、高度のセキュリティを確保した通信サービスと、そうでない通信サービスとを切替えて運用できるようなアクセスポイントは実現されていない。

【0008】そこで、本発明の目的は、無線通信パケットの暗号化機能を利用して、高度のセキュリティを確保した通信サービスと、そうでない通信サービスとを切替えて運用できるような多様な通信サービス機能を実現することにある。

【0009】

【課題を解決するための手段】本発明の観点は、無線通信パケット毎に、暗号化機能（例えばWEP）の適用の有無（オン/オフ）をチェックし、当該適用状態に基づいてパケットの通信サービスを決定できる機能を備えたアクセスポイントのような電子機器に関する。

【0010】具体的には、本電子機器は、無線通信機能を有する端末装置と、前記端末装置との間で無線データ通信の中継機能を有し、端末装置から送信されるパケット単位のデータを受信する受信手段と、受信手段により受信されたパケットに無線通信用の暗号化機能が適用されているか否かを判別する判別手段と、判別手段の判別

結果に基づいて、パケットの通信処理を決定する通信処理手段とを備えたものである。

【0011】このような構成であれば、暗号化機能の適用または非適用のいずれの無線通信パケットを取り扱うことができるアクセスポイントの運用を実現することができる。更に、無線通信パケット毎に、暗号化機能の適用または非適用に応じて、例えば高度のセキュリティを確保した通信サービスと、そうでない通信サービスとを切替えて運用できる効果がある。

【0012】

【発明の実施の形態】以下図面を参照して、本発明の実施の形態を説明する。

【0013】（システムの構成）図1は、同実施形態に関するアクセスポイントのシステム10の構成を示すブロック図である。本システム10は、無線LANや有線LANのデータ通信を中継する基地局に相当する設備である。換言すれば、本システム10は、無線通信機能を有する無線端末とネットワーク、特に無線LAN、有線LAN、インターネットとのデータ通信の中継機能を備えたネットワーク接続装置に相当する。

【0014】図1において、CPU11は、メモリ13上にロードされたプログラムを実行し、無線LANや有線LANの中継機能を実現する。具体的には、CPU11は、無線LANコントローラ14、有線LAN（例えばイーサネット：登録商標）コントローラ15、及びATM（非同期転送モード）コントローラ16を制御する。

【0015】バスブリッジ12は、CPU11の通信と、無線LANコントローラ14、有線LANコントローラ15、ATMコントローラ16のそれぞれの通信と、メモリ13の通信との中継を実行する。換言すれば、バスブリッジ12は、CPUバス、メモリバス、及び各コントローラ14、15、16に接続された例えばPCIバスを監視し、各バス間のデータの送受信を管理する。

【0016】メモリ13は、CPU11の動作を制御するプログラム以外に、無線LANコントローラ14、有線LANコントローラ15、ATMコントローラ16のそれぞれの間で通信される通信パケット（以下単にパケットと呼ぶ）の一時的格納領域として機能する。

【0017】無線LANコントローラ14は、例えばIEEE802.11b規格に準拠したものであり、無線LANポートに接続された無線端末100との無線データ通信を管理する。無線端末100は、無線通信機能を有するパーソナルコンピュータや、携帯電話機も含むモバイル情報機器等に相当する。有線LANコントローラ15は、有線LANポートの通信を管理し、オフィス等の有線LANで構成された例えば基幹ネットワークとのデータ通信を管理する。ATMコントローラ16は、ATMポートの通信を管理し、例えばインターネットとの

データ通信を管理する。

【0018】（ソフトウェア構成）次に、図2を参照して、同実施形態のシステム10のソフトウェア構成を説明する。

【0019】本システムは、LAN側システムと、WAN（wide area network）側システムとに大別される。LAN側システムのソフトウェアとしては、ブリッジ処理部21、MAC（media access control）アドレス管理テーブル22、無線LAN（WLAN）パケット処理部23、無線LANDライバ24、有線LANDライバ25、IP（internet protocol）処理部26、及びユーザ認証処理部27である。

【0020】ブリッジ処理部21は、WLANパケット処理部23を経由して無線LANDライバ24、有線LANDライバ25、IP処理部26のそれぞれの間で通信パケットの転送処理を制御する。また、ブリッジ処理部21は、MACアドレス管理テーブル22をアクセスし、MACアドレスと通信ポートとの関連付け情報を管理する。MACアドレス管理テーブル22は、通信パケットのMACアドレス（送信元と宛先）を管理するための管理テーブルを構成し、同実施形態では無線端末100及び通信相手端末が接続されている通信ポートを指定するための関係情報を提供するためのデータベースである。

【0021】WLANパケット処理部23は、無線LANDライバ24が受信した通信パケット（無線LANパケット）の暗号化機能（WEP）の適用又は非適用をチェックする機能を有する（後述する）。また、WLANパケット処理部23は、MACアドレス管理テーブル22を参照し、通信パケットの転送の可否を制御する。

【0022】無線LANDライバ24は、無線端末100との無線データ通信を制御する。無線LANDライバ24は、暗号化機能（WEP）の適用がなされた通信パケットの暗号化データを復号化する機能を有する。有線LANDライバ25は、有線LANを介して接続する端末（パーソナルコンピュータなど）とのデータ通信を制御する。

【0023】IP（internet protocol）処理部26は、ブリッジ処理部21とWAN側システム28との間でIPパケットの転送処理を制御する。また、IP処理部26は、当該システム（機器）自身に割り当てられているIPアドレスを確認し、必要に応じてユーザ認証処理部27や、他の通信プロトコル制御処理部にパケット処理を受け渡す機能を有する。ユーザ認証処理部27は、IP処理部26と連携して、無線端末100が要求する認証処理を実行する。

【0024】WAN側システム28としては、例えばPPP（point to point protocol）ドライバ29、RFC（request for comments）1483ドライバ30、及びATMドライバ31を有し、インターネットに接続し

ている。PPPドライバ29は、ATMドライバ31を経由して接続したサーバとの通信を制御する。RFC1483ドライバ30は、PPPドライバ29と、ATMドライバ31との間の通信を制御する。ATMドライバ31は、ATMコントローラ16を制御し、インターネットとの間で通信パケットの転送制御を実行する。

【0025】（通信パケットの通信処理手順）以下主として図2、図3のフローチャート及び図4を参照して、同実施形態のアクセスポイントと無線端末との通信手順を説明する。

【0026】同実施形態では、無線端末100は、アクセスポイントに接続し、通信パケットを送信する場合に、暗号化機能の適用又は非適用を選択できる機能を備えていることを想定する。具体的には、図4に示すように、通信パケット40は、大別してMACアドレスなどが記録されるヘッダ部41と、データペイロード部42とからなる。同実施形態では、暗号化機能として、例えばIEEE802.11による無線LAN規格のオプション機能として規定されたWEP（wired equivalent privacy）機能を想定する。通信パケット40は、WEP機能の適用又は非適用を示す識別情報として、ヘッダ部41に含まれるWEPフラグ410を有する。即ち、WEP機能が適用されて、データペイロード部42のデータが暗号化データの場合には、WEPフラグ410がオン（論理「1」）にセットされる。また、WEP機能が非適用の場合には、WEPフラグ410はオフ状態（論理「0」）である。

【0027】無線端末100とアクセスポイントとの無線通信は、無線端末100の通信ソフトウェアが起動することにより確立する。無線LANドライバ24は、無線端末100から送信された通信パケットを受信すると、WLANパケット処理部23に引き渡す。WLANパケット処理部23は、図3に示すように、受信した通信パケットにはWEP機能が適用されているか否かを判別する（ステップS1）。即ち、前述したように、WLANパケット処理部23は、ヘッダ部41に含まれるWEPフラグ410のオン/オフ状態をチェックすることにより、WEP機能の適用又は非適用を判別する。

【0028】WLANパケット処理部23は、判定結果によりWEP機能が非適用の通信パケットの場合には、MACアドレス管理テーブル22を参照し、通信パケットの宛先MACアドレスが有線LANポートに接続されたノードのアドレスに合致するか否かを判定する（ステップS1のNO、S2）。即ち、通信パケットの宛先が、有線LANポートの先に存在するか否かを判定する。この判定結果により通信パケットの宛先が有線LANポートに接続されたLANノードではない場合には、宛先IPアドレスの判定処理に移行する（ステップS2のNO、S3）。

【0029】WLANパケット処理部23は、通信パ

ケットの宛先IPアドレスが、当該システム（機器）自身に割り当てられているIPアドレスであるか否かを判定する。この判定結果により通信パケットの宛先IPアドレスが割り当てられていない場合には、WLANパケット処理部23は、当該通信パケット（受信パケット）を破棄する（転送禁止）処理を実行する（ステップS3のNO、S4）。

【0030】一方、WLANパケット処理部23は、受信した通信パケットにWEP機能が適用されている場合には、当該通信パケット（受信パケット）をブリッジ処理部21に渡す（ステップS1のYES、S5）。ここで、通信パケットの暗号化データ（42）は、無線LANドライバ24により元のデータに復号化される。即ち、WEP機能は、パケットのデータを暗号化して、無線端末とアクセスポイント間の無線通信におけるデータのセキュリティ（第三者による傍受の回避機能）を高めることである。なお、当然ながら、無線LANドライバ24はWEP機能の復号化処理のみを実行するだけで、元のデータ自体が暗号化されている場合でもその復号化処理を実行することはない。

【0031】同実施形態では、ブリッジ処理部21は、MACアドレス管理テーブル22を参照し、WEP機能が適用された通信パケットの宛先MACアドレスが、有線LANポートに接続された先に存在していれば、無条件に当該通信パケットを有線LANポートに転送する。要するに、WEP機能が適用された通信パケットのみが、有線LANポートに転送することが許可される。

【0032】また、WLANパケット処理部23は、受信した通信パケットにはWEP機能が非適用の場合でも、宛先MACアドレスが、有線LANポートに接続された先に存在していれば、当該通信パケット（受信パケット）をブリッジ処理部21に渡す（ステップS2のYES、S5）。さらに、WLANパケット処理部23は、受信した通信パケットにはWEP機能が非適用の場合でも、宛先IPアドレスが割り当てられたIPアドレスに含まれていれば、当該通信パケット（受信パケット）をブリッジ処理部21に渡す（ステップS3のYES、S5）。

【0033】以上要するに同実施形態によれば、無線端末100から送信された通信パケットのWEP適用又は非適用に応じて、WLANパケット処理部23及びブリッジ処理部21により、当該通信パケットの通信処理を切替えることができる。具体的には、WEP機能が適用された通信パケットについては、有線LANポートに接続された有線LANに転送し、非適用の場合には破棄するなど、高度のセキュリティを確保した通信サービスを実現できる。一方、WEP機能が非適用の場合でも、宛先MACアドレスのチェックのみで、有線LANポートに接続された有線LANに転送することができる。また、宛先IPアドレスのチェックのみで、当該通信パ

10

20

30

40

50

ットをIP処理部26に転送することができる。IP処理部26は、例えばATMドライバ31を経由してインターネットに接続された宛先ノードに当該通信パケットを送信する処理を実行できる。

【0034】従って、WEP機能の適用又は非適用により通信サービスの固定化を回避し、高度のセキュリティを確保した通信サービスや、そうでない通信サービスなど多様な通信サービスを実現することが可能となる。

【0035】(変形例1)図5は、同実施形態の変形例に関するフローチャートである。本変形例は、WEP機能が非適用の場合でも、当該通信パケットが認証用パケットの場合には、IP処理部26を経由してユーザ認証処理部27に転送する通信サービス機能に関する。以下、具体的に説明する。

【0036】WLANパケット処理部23は、図5に示すように、受信した通信パケットにはWEP機能が適用されているか否かを判別する(ステップS10)。判別結果によりWEP機能が非適用の通信パケットの場合には、当該通信パケットが認証用パケットであるか否かを判定する(ステップS10のNO, S11)。この判定結果により、通信パケットが認証用パケットでなければ、WLANパケット処理部23は、当該通信パケット(受信パケット)を破棄する(転送禁止)処理を実行する(ステップS11のNO, S12)。

【0037】一方、WLANパケット処理部23は、受信した通信パケットにWEP機能が適用されている場合には、当該通信パケット(受信パケット)をブリッジ処理部21に渡す(ステップS10のYES, S13)。ここで、WLANパケット処理部23は、受信した通信パケットにはWEP機能が非適用の場合でも、認証用パケットの場合には、当該通信パケット(受信パケット)をブリッジ処理部21に渡す(ステップS11のYES, S13)。

【0038】ブリッジ処理部21は、MACアドレス管理テーブル22を参照し、WEP機能が適用された通信パケットの宛先MACアドレスが、有線LANポートに接続された先に存在していれば、無条件に当該通信パケットを有線LANポートに転送する。要するに、WEP機能が適用された通信パケットのみが、有線LANポートに転送することが許可される。

【0039】一方、ブリッジ処理部21は、WEP機能が非適用の場合でも、当該通信パケットが認証用パケットであればIP処理部26に転送する。これにより、ユーザ認証処理部27は、IP処理部26から渡される認証用パケットにより、無線端末100が要求する認証処理を実行する。要するに、WEP機能が非適用の場合でも、無線端末100が要求する認証処理については無条件に実行する通信サービスを実現できる。

【0040】(変形例2)図6は、同実施形態の変形例に関するフローチャートである。本変形例は、特に有線

LANに接続されているプリンタや共有ファイルのような資源の利用を許可されたユーザと、その使用を制限されたユーザ(ゲスト権限の利用者)とを、通信パケットのWEPの適用又は非適用で判別する通信サービス機能に関する。以下、具体的に説明する。

【0041】WLANパケット処理部23は、図6に示すように、受信した通信パケットにはWEP機能が適用されているか否かを判別する(ステップS20)。判別結果により通信パケットにWEP機能が適用されている場合には、当該通信パケットをブリッジ処理部21に渡す(ステップS20のYES, S23)。ブリッジ処理部21は、MACアドレス管理テーブル22を参照し、WEP機能が適用された通信パケットの宛先MACアドレスが、有線LANポートに接続された先に存在していれば、無条件に当該通信パケットを有線LANポートに転送する。これにより、WEP機能が適用した通信パケットを送信した無線端末のユーザは、有線LANに接続されているプリンタや共有ファイルを利用することができる。

【0042】一方、WLANパケット処理部23は、判定結果によりWEP機能が非適用の通信パケットの場合には、MACアドレス管理テーブル22を参照し、通信パケットの宛先MACアドレスが有線LANポートに接続されたノードのアドレスに合致するか否かを判定する(ステップS20のNO, S21)。この判定結果により通信パケットの宛先が有線LANポートに接続されたノードの場合には、WLANパケット処理部23は、当該通信パケットを破棄する処理を実行する(ステップS21のYES, S22)。

【0043】ここで、通信パケットの宛先IPアドレスが、当該システム(機器)自身に割り当てられているIPアドレスである場合に、WLANパケット処理部23は、当該通信パケットをブリッジ処理部21に渡す。IP処理部26は、ブリッジ処理部21からATMドライバ31を経由して、インターネットに接続された宛先ノードに当該通信パケットを送信する処理を実行する(ステップS21のNO, S24のYES)。

【0044】要するに本変形例では、通信パケットのWEPの適用又は非適用に応じて、有線LANに接続されているプリンタや共有ファイルのような資源の利用を許可されたユーザと、その使用を制限されたユーザ(ゲスト権限の利用者)とを区別する通信サービスを実現することができる。この場合、ゲスト権限の利用者は、有線LANに接続されているプリンタや共有ファイルのような資源を利用できないが、インターネットへの接続サービスを受けることができる。

【0045】

【発明の効果】以上詳述したように本発明によれば、特に無線端末とのネットワーク中継機能を備えた電子機器において、無線通信パケットの暗号化機能を利用して、

高度のセキュリティを確保した通信サービスと、そうでない通信サービスを切替えて運用できるような多様な通信サービス機能を実現することができる。

【図面の簡単な説明】

【図1】本発明の実施形態に関するシステムのハードウェア構成を示すブロック図。

【図2】同実施形態に関するソフトウェア構成を説明するための図。

【図3】同実施形態に関するパケット送受信手順を説明するためのフローチャート。

【図4】同実施形態に関する通信パケットのフォーマットを説明するための図。

【図5】同実施形態の変形例1に関するパケット送受信手順を説明するためのフローチャート。

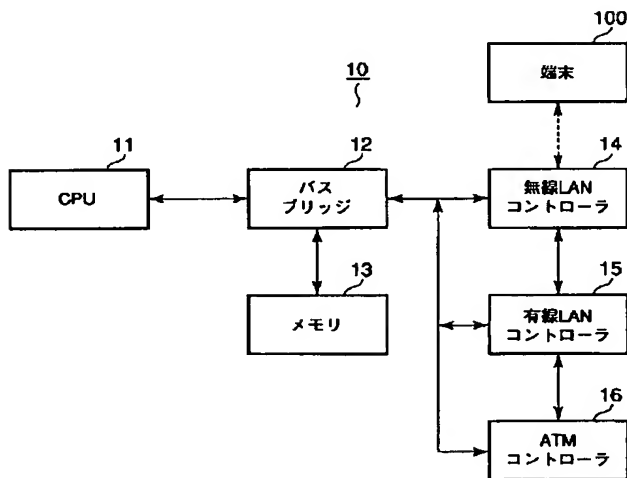
【図6】同実施形態の変形例2に関するパケット送受信手順を説明するためのフローチャート。

【符号の説明】

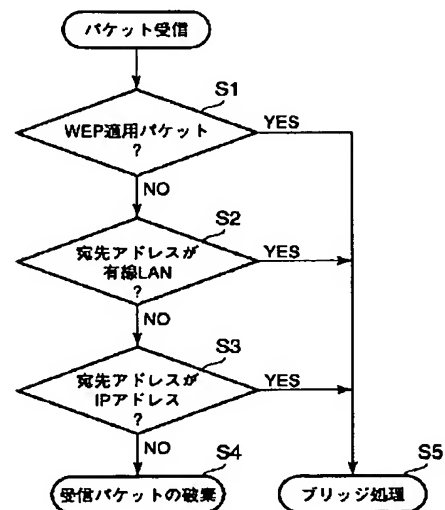
*

- * 10…アクセスポイント
- 11…CPU
- 12…バスブリッジ
- 13…メモリ
- 14…無線LANコントローラ
- 15…有線LANコントローラ
- 16…ATMコントローラ
- 21…ブリッジ処理部
- 22…MACアドレス管理テーブル
- 23…無線LANパケット処理部
- 24…無線LANドライバ
- 25…有線LANドライバ
- 26…IP処理部
- 27…ユーザ認証処理部
- 28…WAN側システム
- 100…無線端末

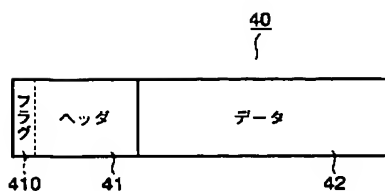
【図1】



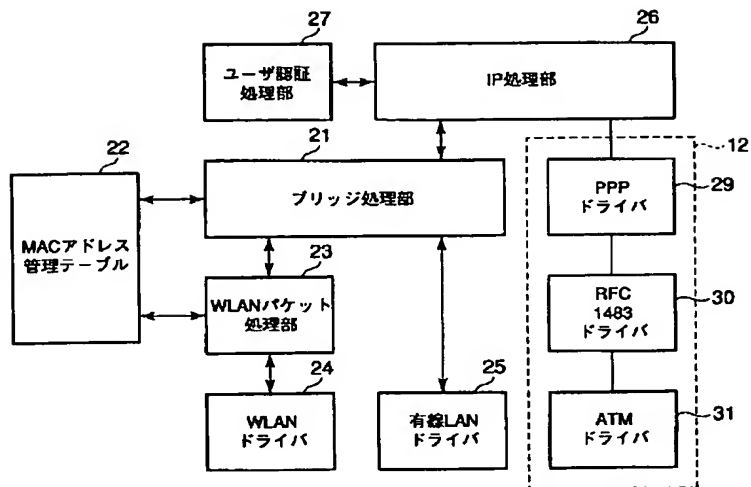
【図3】



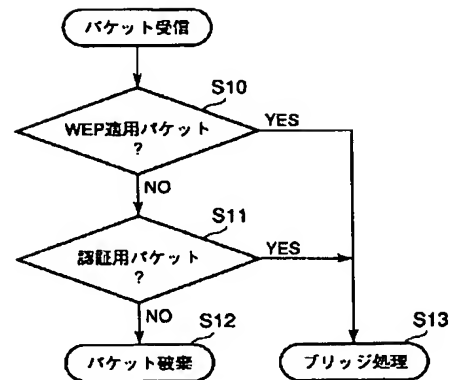
【図4】



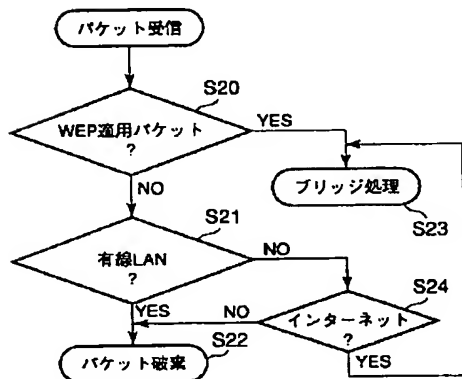
【図2】



【図5】



【図6】



フロントページの続き

Fターム(参考) 5K033 AA08 DA05 DA19 DB19 EC04
 5K067 AA21 AA30 BB21 CC08 DD17
 EE02 EE10 HH36 KK13